

Filed Under Seal

EXHIBIT G

‘MV Privacy’ Talking Points (Mar. 2023)

Notes on Framing:

- The metaverse [[HYPERLINK](https://docs.google.com/document/d/1ZK1Hv9yEdQFaBuScyqUR7bu4P1_-ZnZBubn-UScWCYM/edit) "https://docs.google.com/document/d/1ZK1Hv9yEdQFaBuScyqUR7bu4P1_-ZnZBubn-UScWCYM/edit" \l "bookmark=id.a9l45qx770x7" \h] for policy elites starts with describing the **value** that Meta provides people and their communities. This is closely followed by our commitment to **responsibility** as we help build the metaverse.
- Meta will deliver value and act responsibly by creating opportunities for as many people as possible through **collaboration** with others, **transparency** about what we are building and how we will make money, and **outside investments** in those who are also helping build the metaverse.

Table of Contents

[TOC \h \u \z \n \t "Heading 1,1,Heading 2,2,Heading 3,3,Heading 4,4,Heading 5,5,Heading 6,6,"]

Approach to privacy between FoA and RL products

1. Similarities and differences in approach to privacy between FoA and RL products

Is there any difference in approach to privacy between FoA and RL products?

- **Broad Consistency across Meta with a tailored approach to individual products:**
 - We aim not to surprise our users and that we deliver privacy in line with their expectations. We believe people should be in control and therefore we provide the controls and features that enable you to do that. This commitment is consistent across our company and products, in fact our [[HYPERLINK "https://www.facebook.com/privacy/policy"](https://www.facebook.com/privacy/policy)] covers our key products, from Facebook, to Instagram to Meta Platform Technologies Products.
 - At the same time, we're building new hardware at Reality Labs. For some products we need to take a tailored approach for each new form factor. For example, our hardware products may require special privacy by design features that are not relevant to our Family of Apps such as considering bystander notifications. For this reason, some of our products are subject to [[HYPERLINK "https://www.meta.com/legal/quest/privacy-policy/?utm_source=l.facebook.com&utm_medium=oculusredirect"](https://www.meta.com/legal/quest/privacy-policy/?utm_source=l.facebook.com&utm_medium=oculusredirect)] , which complement the Meta Privacy Policy by explaining the additional information we process to support MPT Products and providing more details about how we process that information.
- **Responsible Innovation Principles / Privacy by Design:**
 - Privacy in the metaverse will be informed by expectations we develop from the physical world and by privacy norms and experiences in today's internet. In essence, basic privacy principles (which are technology neutral) will apply to the metaverse.
 - However, unique and novel characteristics of the metaverse, such as immersion and presence, may raise a small number of new privacy considerations.
 - Novel issues such as augmented reality's impact on bystanders (or people around our devices when they're in use), avatar identity and security, and privacy in immersive environments require collaborative and open discussion with stakeholders across the ecosystem. Responsible innovation demands that developers build the metaverse with privacy in mind from the ground up.
 - Our Responsible Innovation Principles, launched in September 2020, define our approach and philosophy to product development across all our metaverse technologies. They are a clear north star and are designed to ensure that privacy is always top of mind. They are especially relevant when we consider people's privacy priorities and experiences in immersive environments.
 - The four principles are:
 - (1) **Put people first** = by designing people-first technology that starts with being responsible stewards of people's data

- Example: While we take precautions with all data, we take specific precautions with data that could be considered sensitive. On the Meta Quest Pro, for example, when you choose to enable eye tracking, software on the headset analyzes infrared images of your eyes ("raw image data") to create an estimate of where your eyes are looking in VR ("abstracted gaze data"). This estimation is done on your device in real time as your eyes move. Raw image data is processed directly on the headset and deleted from the headset after the abstracted gaze data is generated. Raw image data is not collected or stored on Meta servers; nor is it shared with any third parties. A user can choose to share abstracted gaze data with an app, which may be offered either by Meta or a 3P, in order to use the eye tracking feature in the app.
- (2) **Provide controls that matter** = so that people can exercise choice over how their data is used and how to personalize their experiences:
 - Examples:
 - We offer clear and simplified controls to users in respect of their preferences for how to use their data including for optimizing user experience.
 - VR privacy controls include:
 - Active Status - ability to turn on/off when you are active in VR
 - Activity - ability to toggle public/your followers/only me for the apps you use and your activity (e.g. achievements and high scores)
 - Private Profile - ability to turn on/off private profile which allows people to control whether they require approval for others to follow them
 - Upon device setup, users can choose how public and social they want to be.
 - Eye/hand tracking and Natural Facial Expressions are all opt-in. We also make it easy for you to turn eye tracking/NFE on/off from the Quick Settings bar in VR. "You can pause the eye tracking and Natural Facial Expressions features at any time straight from the Quick Settings bar, without having to navigate back to the main Settings menu."
- (3) **Consider everyone** = when developing our products we do so in a way that includes stakeholders that represent the interests of our users
 - Example: Meta Quest has an Accessibility tab in the Settings menu including Color Correction, which helps people who are color blind more easily distinguish colors within the headset, and Adjust Height, a feature that gives people the option to view VR in a "standing" mode even if they're physically seated.
 - Example: Meta Avatars offer over one quintillion combinations of options for users to represent themselves in VR and across our

Family of Apps. We consult with relevant experts and community members to design Avatar assets for a diverse and global user base. For example, we have done research with people with disabilities to ensure that as we continue to add more options over time, our avatar options across the Family of Apps feel authentic to the people who use them.

- (4) **Never surprise people** = we aim to be as transparent as possible about how we use people's data and about how we do business
 - Example: We clearly articulate how we collect and use data about people and design our metaverse facing products from the ground up to match user expectations as closely as possible. We have researchers dedicated to trust, privacy, and social acceptability working both RL-wide and in product verticals who:
 - ❖ explore users' mental models and ways to educate users about novel tech and novel data types
 - ❖ study new interaction models and best practices for user transparency and control, including identifying where users' needs may differ for extended reality vs. other tech
 - ❖ evaluate products and features based on those needs and expectations to ensure we ship products that facilitate user trust
 - ❖ study bystander needs and expectations to inform features that protect bystander privacy and user education that encourages responsible use

- **Collaboration:**

- We shouldn't be the only leaders in metaverse privacy. The metaverse won't be built, operated or governed by any one company or institution. We are committed to privacy and responsible innovation and are supportive of collaborative efforts on the system design of the metaverse. We are working with international bodies and organizations such as the Metaverse Standards Forum, the World Economic Forum and others to explore standards for the metaverse, including in privacy.
- We use co-design to explore metaverse privacy with policymakers, academics and civil society and generate new insights on transparency and control for data. (e.g. [[HYPERLINK](https://fb.workplace.com/groups/691058377896583/permalink/1785049801830763/) "https://fb.workplace.com/groups/691058377896583/permalink/1785049801830763/" \h], [[HYPERLINK](https://fb.workplace.com/groups/691058377896583/permalink/1717133448622399/) "https://fb.workplace.com/groups/691058377896583/permalink/1717133448622399/" \h], [[HYPERLINK](https://l.workplace.com/l.php?u=https%3A%2F%2Fabout.fb.com%2Fnews%2F2023%2F02%2Flaunching-metas-first-pan-european-design-challenge-on-safer-internet-day%2F&h=AT0kjlafCOPwE0tWT3oHF0J5qpND2KFmQOLa8dxniEJvUj5fmvGq6RkwBkeEorIWf5vsfGBKxqu__K9VT-W9mL6-) "https://l.workplace.com/l.php?u=https%3A%2F%2Fabout.fb.com%2Fnews%2F2023%2F02%2Flaunching-metas-first-pan-european-design-challenge-on-safer-internet-day%2F&h=AT0kjlafCOPwE0tWT3oHF0J5qpND2KFmQOLa8dxniEJvUj5fmvGq6RkwBkeEorIWf5vsfGBKxqu__K9VT-W9mL6-

qfsujGeBiR3lqFpWZSWGQDquNA9iQ93yYKmORXjwKJhq7LaDuxkbQbWbsjpK
80EZyKbjsUtTh5IWg" \h))

- **Transparency**

- We understand that transparency is a key component of building trust in novel products and services and empowering people to make informed choices about our products. That's why we are committed to developing best practices around transparency which balance clarity and comprehensiveness with good user experiences to maximize people's engagement with the information.
- We approach transparency in the metaverse from many different angles including:
 - (i) informing the public at large via our publications on how we treat data in our product
 - (ii) layering the information via contextual, "just in time" user notifications with links to further information, as we currently do across our products and which we believe remains valid typically in immersive environments
 - (iii) fostering accessibility via targeted educational resources and a variety of different media (from blogs to short videos and white papers) for improved understandability across our user base - this will be all the more important for novel features for the metaverse
 - (iv) co-designing for new and adaptive methods of information.
- In that regard, in addition to building a series of tools to help our users understand how we collect and process data in our products, we believe that tools to help users understand how platforms collect and process data should be industry standard.
- We understand that transparency is a key component of building trust in novel products and services. That's why we are committed to developing best practices around transparency which balance clarity and comprehensiveness with good user experiences to maximize people's engagement with the information
- In the Meta Quest Privacy Center users can control their privacy settings including who can see their active status, whether their profile is private or public, and the ability to hide activity for specific apps. Users can also view information that we collect when they use the Meta Quest headset and app, download information they provided to us as part of their use of Meta in case they want to take it to another service, delete Meta Quest Move data, delete Meta and Horizon data, and link/unlink Meta Accounts through Accounts Center.

Importance of privacy in metaverse vision and Reality Labs product execution

2. The importance of privacy in our metaverse vision and Reality Labs product execution

What is the importance of privacy in our metaverse vision?

- We believe that privacy is a foundational condition of building the metaverse.
- As the next computing platform, spatial computing allows for more seamless interaction between people and technology. The technology should innately work for people, and people should be in control of their privacy in a way that they would expect in immersive physical environments.
- We want people to feel comfortable to use our technologies in their everyday lives, and privacy is core to that.
- Our metaverse vision is built on our Responsible Innovation principles (see above), all four of which are conducive to privacy. The products and services that we are building in Reality Labs are being developed through this lens from day one.

What is the importance of privacy in our RL product execution?

- Privacy is foundational to our metaverse vision. Because we are developing leading and novel edge XR ecosystem products that offer unprecedented opportunities to people, we take this early mover responsibility seriously and take steps internally to ensure that privacy is considered in depth via rigorous processes in the development of all RL products.
- We can't [and don't intend to] build the metaverse alone. That's why we're partnering with experts in government, industry and academia to think through issues and opportunities in the metaverse along the way.
- We also need to involve the human rights and civil rights communities from the start to ensure these technologies are built in a way that's inclusive and empowering.
 - In that regard, we published our first annual human rights [[HYPERLINK "https://about.fb.com/news/2022/07/first-annual-human-rights-report/"](https://about.fb.com/news/2022/07/first-annual-human-rights-report/) \h][[HYPERLINK "https://about.fb.com/news/2022/07/first-annual-human-rights-report/"](https://about.fb.com/news/2022/07/first-annual-human-rights-report/) \h]. As we look to building the metaverse, we are focused on inclusiveness and responsible innovation, and this report helps us do just that, i.e. develop a strong practice for managing evolving human rights risk.

Approach to Privacy in metaverse

3. Our approach to privacy in the metaverse:

- Firstly, experiences in 3D will feel closer to physical world experiences than to 2D world experiences because they share 3 key similarities:
 - Ephemerality - in the metaverse we shift from a written communications' internet in the main to more live, speech-based communications. Our face-to-face conversations will be more transient, like in the physical world.
 - Embodiment - in 3D environments, our presence is embodied through 3D

- avatars that will mirror our facial and body movements in real time.
 - And immersion - we will be virtually sharing a specific space with other people with high fidelity audiovisual and graphic rendering to experience more natural social interactions in shared 3D environments like a conversation with friends in a coffee shop, at home or in a meeting in the workplace.
 - We also wish to emphasize that experiences in the metaverse will be 'additive' to improve familiar experiences, not replace them.
- As we approach conversations around privacy and data governance in the metaverse, we must do so while keeping alive the breadth of experiences it will provide, and limiting the ability for central control, in our view.
- The norms that exist in the physical world are many of the same norms that should exist in the virtual world.
 - For example, in a public space in the physical world, people expect more robust norms, rules and standards than they do in closed spaces – like their home where they have more control over what is said and done.
 - However, when they walk into a restaurant, there's an understood etiquette and you often see rules that govern that space posted by the owner of the space (e.g. no food or drinks permitted or reservation required).
 - Similarly, in virtual reality, users will have comparable expectations that will differ depending on whether they are in a virtual "town square", a restaurant, or their individual house : *"The immediacy of metaverse spaces makes it more likely that this sort of synchronous, ephemeral communication will be far more prevalent than the tangible, text-based communication that dominates much of today's internet. So, in this case, a better place to look for answers may be the existing rules and norms that govern bars in physical reality."* (Nick Clegg,[[HYPERLINK "https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04" \h \]](https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04)).
- The metaverse will be built in part on the next generation of computing and will allow people and technology to interact in new ways far beyond the 2D screens of today. The opportunities created by this new technology are simply enormous for people and have the potential to unlock new opportunities for work, education, and commerce. However, this new form of computing requires the collection of larger volumes of real time data. This creates new privacy challenges and opportunities such as investing in privacy enhancing technologies (PETs).
- Understanding user expectations and giving people meaningful control over their privacy is key to ensuring that these new technologies are built responsibly. That

is why we conduct user research, build RL products with data minimisation and purpose limitation practices, and offer simplified meaningful privacy controls for people.

- All RL products go through a rigorous internal privacy review process to ensure that at all stages the data governance and management practices behind RL products are secure and privacy first.

Personal Data Collection

4. Personal Data Collection

There is a lot of concern around how Meta will govern data collection and privacy in the metaverse. How will data be collected, who will collect the data and who will have access to the data?

- **Novel inputs / new sensors**
 - With the development of new technologies, particularly VR and AR devices, comes the development of new sensors and novel data inputs (data collection opportunities).
 - An example of a feature powered by novel data input would be [[HYPERLINK "https://drive.google.com/file/d/1_qcPFLXwY8JdNE1M1C-dmk-avaQrWnP0/view?usp=sharing" \h](https://drive.google.com/file/d/1_qcPFLXwY8JdNE1M1C-dmk-avaQrWnP0/view?usp=sharing)] ([[HYPERLINK "https://drive.google.com/drive/folders/1Go5029jmLKq-10lzoJpiM3CdnN622k5e?usp=share_link" \h](https://drive.google.com/drive/folders/1Go5029jmLKq-10lzoJpiM3CdnN622k5e?usp=share_link)]) as seen in the Meta Quest Pro. Eye tracking has the potential to increase the feeling of presence for users in VR by making a user's avatar's eye contact and facial expressions look more natural – like being able to blink or make eye contact with other people. Eye tracking carries certain concerns, that can be mitigated by privacy-protecting measures. An example of such measures include on-device processing to limit what eye tracking data leaves the device (i.e., raw image data is processed on device and not stored or shared to Meta or third parties), but users can choose to share abstracted eye gaze data with an app in order to use the eye tracking feature in the app. Additionally, developers of 3rd party apps on the Meta Quest platform must comply with our Developer Data Use Policy, which outlines permitted and prohibited use cases of data.
 - When it comes to novel data types and new sensors, the industry should work towards common and harmonized practices and standards that ensure the privacy of people across the metaverse.

- For instance, we are committed to participating in the Metaverse Standards Forum, the XR Association and the World Economic Forum's work to open dialogue and collaboration in this area.
- We welcome further cooperation from governments, industry, academic, developers, technical community, and other stakeholders including civil society organizations. Collaborative discussions with regulators are needed for instance to provide guidance that will foster best privacy practices and support user education and awareness on novel data types and new sensors in the metaverse. It is only through collective action and multi stakeholder collaboration that we will be able to ensure the right standard for people in future across the
- **How information will flow in the metaverse**
 - Like today's internet, the metaverse will be a set of technologies, platforms, and products. It won't be built, operated or governed by Meta or any other one company or institution alone.
 - We are investing in building a spatial computing ecosystem to connect many different developers, creators and users. There are several different ways we can think about the data that is generated in the metaverse to start to understand how information will move and be shared across.
 - First, there is the data that users choose to share directly with services in metaverse so that they can provide personalized and functional experiences
 - Second, users may choose to further share their data with third parties that can enhance and extend their metaverse experiences.
 - And finally, there is the collective insight of data patterns that tell us how the metaverse is being used at a macro level. For us, that will be how people are using our technologies collectively and the opportunity to share common anonymous or pseudonymous insights at scale.

Anonymous access to Meta's XR technologies

5. Why doesn't Meta provide anonymous access to its XR technologies?

- It is no longer necessary for people to access our XR technologies via a Facebook account. In August 2022, we rolled out Meta accounts. Users can establish a Meta account with an email, are not obligated to use their real name, and can choose whether or not they want to access connected experiences with Facebook and Instagram in VR. These accounts offer people the option to explore their different aspects of their identity (via the profile layer – username, display name, avatar, etc) without it being attached to other parts of their life (i.e., personal life vs work life).

- An example of the importance of user experience consistency can be seen in user avatars, digital renderings of themselves in XR spaces. People take time to build their avatars and have told us that they want to carry an interoperable avatar across surfaces and experiences. If a user chooses, they can sync their avatar across their Horizon Profile and linked Facebook and Instagram accounts, enabling them to carry a persistent visual identity with them across surfaces and experiences.
- Our identity structure allows people the flexibility to be who they want in the metaverse- even if that's different from how they appear in everyday life - while still upholding safety on our platform. For example, we may share integrity signals across accounts for safety and security purposes.

End-to-end encryption support

6. What parts of the metaverse will have end-to-end encryption support?

- We have successfully rolled out E2EE across Whatsapp in our Family of Apps to offer people more control, more privacy and greater security. E2EE means that Meta and no third party other than the sender and recipient of a message cannot see the content of encrypted messages nor do we process the content of those messages. It has proven a useful tool to ensure the safety and security of people in messaging scenarios.
- The metaverse is still nascent and it is yet to be seen where E2EE will be most useful, however we can already imagine scenarios where it would be a useful tool in other contexts.
- We know that people are concerned about their privacy when it comes to direct messages, and they want to be in control of that. We also know that unsolicited and abusive messages are some things that people want remedies for and may potentially wish to flag. In E2EE both the sender and receiver have access to the content of messages, but Meta does not, but users can choose to share that content with Meta to flag inappropriate conduct. This goes back to offering controls that matter within our Responsible Innovation Principles.

Sensitive data

7. How do you ensure that developers do not gain access to data that may be considered sensitive via APIs? When such data must be shared to enable product functionality, how do you ensure it is not exposed further?

- We have strict privacy and security standards that apps must meet in order to be accepted into the Meta Quest Store and App Lab. We conduct a comprehensive security

review process that includes malware scanning, quality assurance checks and verifying that apps follow the technical standards (or Virtual Reality Check guidelines) we publish.

- Developers must comply with the [HYPERLINK "<https://developer.oculus.com/policy/data-use/>" \h], which outlines how developers may use user data and the safeguards they need to have in place to protect this data.
- We perform regular checks to ensure that developers are complying with our policies. For example, as part of our annual [HYPERLINK "<https://developers.facebook.com/docs/development/maintaining-data-access/data-use-checkup/>" \h], all developers are required to certify that their API access and data use comply with our [HYPERLINK "<https://developers.facebook.com/devpolicy/>" \h] and [HYPERLINK "<https://developers.facebook.com/devpolicy/>" \h]. Failure to do so will result in developers losing API access and their apps will be deactivated.

Youth Privacy & Safety

8. Given that youth privacy and safety is top of mind generally (and, in particular, with respect to Horizon Worlds), how is Meta addressing these issues?

Ensuring young people have age appropriate experiences across all Meta services is a priority. Meta has significantly evolved our approach to protecting young people - we apply a holistic lens to examine privacy, safety & wellbeing, and empower parents and teens with tools and resources to help our teen users develop safe habits in virtual spaces.

We have developed a number of safety tools to help people feel comfortable in Horizon Worlds. As well as the usual mute, block and report functions, we have:

- Personal Boundary: this tool prevents avatars from coming within a 4 foot distance of each other, creating more personal space for people and making it easier to avoid unwanted interactions. We've rolled out Personal Boundary as always on, by default, because we think its important to help set virtual norms
- Fade: to discourage players from sticking their hand into other player's avatar, the avatar someone is trying to touch will fade away; if one user tries to invade someone's person space, users will fade out and appear invisible so the presence is not invaded
- Voice Modes: Voice Mode allows you to choose how you hear people who aren't on your friends list, including the option to not hear unwanted conversations at all. By default, you'll hear all nearby users at the same volume, but with Voice Mode, you can easily switch to Garbled Voices, in which non-friends' voices come across as unintelligible, friendly sounds.
- Dedicated 'Community Guides' who are present across Horizon worlds to welcome players and show them around, encourage positive behavior and point users to available safety tools. They can also take integrity actions against disruptive users - including

warning and kicking the user and reporting them to our trained reviewers for further actioning, up to and including suspension and account disablement

- Live Moderators: who are routed to where a potential incident might be happening in real time, based on integrity signals from players (mute/ block/ report) and can remove offenders from a space and report them for further actions

At Meta, we take a multi-layered and comprehensive approach to providing protections for all users, and in particular teens. For example, we provide and continue to iterate on platform-level safety and privacy tools for all users, especially teens. Parental supervision in VR, which launched during this past summer, plays an important role in our approach to protecting teens and is now available in the Meta Quest companion app, in VR, and on the web through Family Center.

- Once a parent and a teen have linked their accounts, parents have the ability to block specific apps that may be inappropriate for their teen, view the apps their teen owns, view their teen's list of people they follow and people who follow them, view time spent in VR, receive "Purchase Notifications," alerting them when their teen makes a purchase in VR, block Link and Air Link and [New] Developer Mode, and enable and disable social features. Teens will be able to view the controls guardians applied within their account, understand what information is shared with their guardian when parental supervision is set up and receive relevant notifications about any changes. One of the primary principles guiding parental supervision is respect for teen autonomy. We want to promote youth privacy and agency and ensure that they know/are comfortable with what controls are applied. Additionally, we also hope to encourage communication between the teen and guardian.
- We also launched the VR Parent Education Hub this year, linked to on the Safety Center, that helps parents discuss safe VR use with their teens. The Hub includes a Parent's Guide to Meta's VR Parental Supervision Tools from ConnectSafely that provides context about the new VR parental supervision tools and helps parents support their teens with tips for how to conduct themselves in VR now and as they mature.

Use of novel sensor data and AR/VR information for advertising or personalization

9. How does Meta think about the use of novel sensor data or other AR/VR information for advertising or personalization?

[NOT TO BE RAISED UNLESS ASKED: colleagues should follow up afterwards with stakeholders if explicitly asked this question]